2D-05

# エントロピーを用いた類似度評価システムの応用に関する一考察

高田　慎也　元田　敏浩
NTT セキュアプラットフォーム研究所
takada.shinya@lab.ntt.co.jp

## 1.はじめに

類似するファイルを高速かつ高精度に見つけ出すことに対するニーズは高く、こうした分野で使用されるファイル類似度の評価方法としては、例えば、ファイルのエントロピー値を比較することで類似度を測定する方法の研究が盛んに行われている[1][2]。これに対して類似度を評価するファイルを分割し、エントロピー値をファイルの区分ごとに計算し、得られるスペクトルに DP マッチングを施した後に比較することで、より高精度に類似度評価を行う方式を提案してきた。またこの方式の応用として不正バイナリファイルがファイルを搾取するアプリケーションスプーフィングの防止への適用を提案した[6]。一方、ウィルス検知ソフトでは従来のハッシュ値の比較をする方式にヒューリスティックな手法を追加することで、さらに検出率を向上させることが試みられている。本稿ではこうした試みを参考にアプリケーションスプーフィング対策を目的としたシステムの実現方式を検討する。

## 2. エントロピー値の計算方法

エントロピー値は閉域系における順序性の程度の指標値である。エントロピー値の計算方式は、

$$\mathrm{E} = -\sum_{\mathrm{i}=0}^{255} \mathrm{P_i} \log_2(\mathrm{P_i})$$

で定義される。

## 3. これまで検討してきた類似度評価方式

これまで検討してきたエントロピーを用いたファイル類似度評価式について簡単に紹介する。これまでの検討でファイル全体のエントロピー値を使って類似度を評価する方式は、誤検出が多いという結果が得られた。そこでファイルを分割し、区間ごとの差を比較する方式を考案した。

$$\text{類似度(差分平均)} = \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}} |\mathrm{Ex_i} - \mathrm{Ey_i}|}{\mathrm{n}}$$

この式では、比較対象の 2 つのファイルを区分に分割し、各区分での区分エントロピー値をそれぞれ（Exi, Eyi）求め、得られた値の差を取り、これをファイルの最後まで繰り返した後、差分平均を計算することで類似性を評価する。差分平均が 0 の時 2 つのファイルは一致し、差の増大とともに 2 つのファイルの類似度は低くなり、最大値は 8 となる[3][4][5]。

しかしながらこの方式でもエントロピースペクトルに発生するピーク位置のズレが誤差となることが判明したため、スペクトルの比較に DP マッチングを加えた比較方式を導いた。ここで DP マッチングは以下の式で表現される。

$\mathrm{X} = (x_1, x_2, \ldots, x_n)$、$\mathrm{Y} = (y_1, y_2, \ldots, y_n)$について

動的計画法により以下を計算

$$\mathrm{D(X,Y)} = f(n,m)$$

$$f(\mathrm{t,i}) = \|x_t - y_i\| + \min \begin{cases} f(t,t-1)\ X\ Stutter \\ f(t-1,i)Y\ Stutter \\ f(t-1,i-1)\ noStutter \end{cases}$$

$$f(0,0) = 0, \qquad f(t,0) = f(0,i) = \infty$$

DP マッチングを施した結果、Adobe 社 Acrobat の実行形式の Ver9.3.0、Ver10.1.0、Ver11.0.0 のマイナーバージョンのバイナリ抽出を適合率、再現率ともに高スコア(≒100%)で実現することができた[6]。

## 4. 参考としてのウィルス検知ソフトの現状

最近のマルウェアの傾向として少しだけファイルの内容を変えた亜種が作成されるという傾向がある。このため、最近のウィルス対策ソフトでは、ヒューリスティックな機能を導入し、パターンファイルの肥大化防止とプロアクティブな保護の実現を行っている。具体的には、例えば、マルウェアの亜種群に共通する「シグネチャ」を利用し、類似性から亜種を検出するといった対策が施されている。

これを参考に本稿ではアプリケーションスプーフィング防止のため、バイナリファイルの類似性を 3 章の方式で評価することで端末内のバイナリファイルの良性判断を効率的に行うことを目標とする。表 1 は従来のウ

表 1. 従来のウィルス検知ソフトと本検討の方式との比較

| | 従来のハッシュ一致検出型ウィルス検知ソフト | アプリケーションスプーフィングを防止する本検討の方式 |
|---|---|---|
| 処理負荷 | 中<br>ハッシュ計算 | 小<br>エントロピー計算 |
| 1つのパターン（特徴量）のサイズ | 小（ハッシュ値。最大でも1件SHA512=64byte程度） | 中<br>（1件256Byte程度のベクトル値） |
| パターンファイルの種類と更新頻度 | ブラックリスト<br>高 | ホワイトリスト<br>中 |

ィルス検知ソフトと本検討の評価方式を比較したものである。

## 5. 実現方式案

図1は、アプリケーションスプーフィングを防止する本検討の類似度評価システムの機能構成バリエーションを表したものである。図中(1)のファイルアップロード型はバイナリファイルをサーバに送信し、良性バイナリファイルとの類似性を評価し真正性を判定するものである。(2)の特徴量アップロード型はバイナリファイルの区分エントロピー値(以下特徴量と呼ぶ)を端末で計算し、特徴量をサーバに送信し、サーバ側で送られてきた特徴量から良性バイナリファイルとの類似性を評価し真正性を判定するものである。(3)の端末評価型はウィルス検知ソフトと同じように、良性バイナリファイルの特徴量の集合(以下パターンファイルと呼ぶ)を定期的に端末に送信し。端末内のバイナリファイルの特徴量を計算し、これとパターンファイルとの類似性を評価し真正性を判定するものである。

## 6. 実現方式の比較

表2は5章で検討した各実現方式について、NW負荷、サーバ処理負荷、端末処理負荷を比較したものである。(1)ファイルアップロード型はバイナリそのものをNW上でやり取りするため、NW負荷が大きく現実的ではない。一方(3)端末処理型ではNW負荷はパターンファイルの大きさと更新頻度に依存する。特徴量の1件のパターンファイルはハッシュ値のパターンファイルよりサイズが大きいが、1つの特徴量で複数の良性バイナリファイルを抽出できる点、パターンファイルの更新頻度がハッシュ値と比較した場合、低頻度でよい点から許容できる可能性が高い。ただしハッシュ値の場合と同様に経年によりパターンファイルが巨大化していく点については注意が必要である。また、類似度計算を端末で行うため、業務に支障が出ない程度の計算時間で済むよう、端末内のバイナリファイルの特徴量を計算しておくといった工夫が必要である。(2)特徴量アップロード型は3つの案の中で機能的に最もバランスが取れている。端末で当該ファイルの特徴量を計算しサーバに送信(1件256Byte)すればよいため、NW負荷、端末処理負荷とも現実的である。またパターンファイルはサーバ側で管理するため、容量の増加に対してそれほど注意を払う必要はない。さらには類似性評価をサーバ側で行うため、アクセスが集中するケースが想定されるが、特定の、端末共通の特徴量のパターンファイル類似性評価の結果をキャッシュしておくことで処理の効率化を図ることが期待される。

表2. 各実現方式の比較

| | ファイル<br>アップロード型 | 特徴量<br>アップロード型 | 端末評価型 |
|---|---|---|---|
| NW負荷 | 大 | 中 | 中 |
| サーバ処理負荷 | 大 | 中 | 小 |
| 端末処理負荷 | 小 | 中 | 大 |

以上から机上検討では、特徴量アップロード型が、一番実現性が高く、ついで端末評価型が続く結果となった。

## 7.今後の予定

本稿の検討の結果、アプリケーションスプーフィングを防止する目的に対する実現方式としては、ウィルススキャンソフトのような(3)端末型より、(2)特徴量アップロード型の方が、実現性が高くバランスが取れていることが分かった。今後は選定方式の実装を行い、期待通りの傾向が得られるか評価したい。

## 8.参考文献

[1] Mccreight et al. “System and method for entropy-based near-match analysis.” 国際特許 WO2010/107659 A1
[2]Davis et al.Guidance Software “Utilizing Entropy to Identify Undetected Malware”
[3]高田他”類似度を用いたファイル追跡に関する一手法の提案”CSS2012
[4]高田他”ファイルのエントロピー測定による類似度評価の新手法に関する提案” 第60回CSEC研究会
[5]高田他”ファイル類似度評価システムに関する考察”第76回情報処理学会全国大会
[6]高田他”エントロピーとDP Matchingを用いたファイル類似度評価システムに関する考察”第77回情報処理学会全国大会

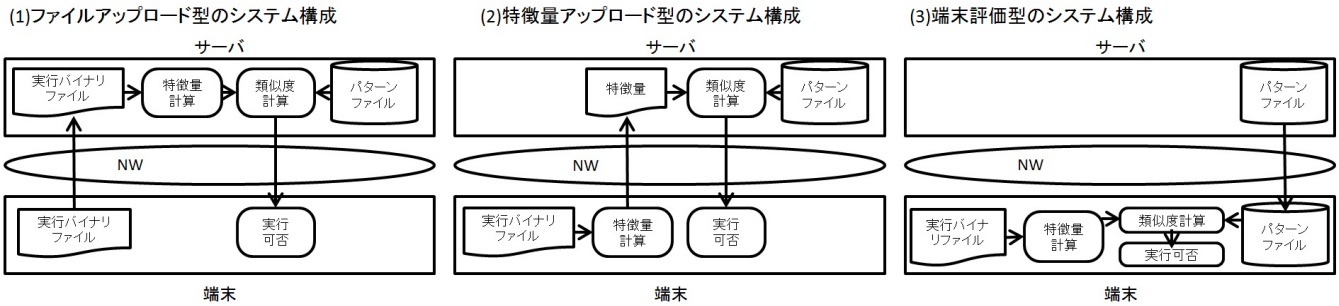


図1. アプリケーションスプーフィングを防止する類似度評価システムの機能構成バリエーション